Journal of Korean Law | Vol. 11, 29-54, December 2011

North Korea and Cyberwarfare: How North Korea's Cyber Attacks Violate the Laws of War

*Tom Papain**

Abstract

On July 4th, 2009, North Korea launched the first of three "DDOS" (Distributed Denial of Service) attacks upon the government and private networks of both the United States and South Korea, effectively flooding these networks with millions of requests from computers which were infected with the North Korean botnet virus "MyDoom." Considered by several experts (including Richard A. Clark) as a precursor of things to come, such attacks are quickly becoming an alternative means of waging war on enemy countries. This is especially true for countries such as North Korea, whose struggling economy and limited resources lead it to attack its enemies in a cheaper - albeit effective – way. In this note, Tom Papain will talk about the laws of war and cyberwar, both in general and as they pertain to the 2009 cyber attacks, and the various treaties which North Korea violated by launching these cyber attacks, including the U.N. Charter Article 2(4), the Geneva Convention, Additional Protocol I, Article 48, and the Hague Cultural Property Convention. In the end, he will talk about possible future developments in the realm of cyberwarfare, including what the International Community should do to combat North Korea's use of cyber weapons, and efforts by the U.S. and Russia to come up with a treaty regulating cyberwarfare.

On July 4th, 2009, the Democratic People's Republic of Korea (hereafter "North Korea"), in response to U.N. sanctions condemning their explosion of a nuclear weapon in May of that year,[1] launched seven short-range ballistic rockets into the Sea of Japan.[2] More surprising, however, was that

* J. D. Candidate, Fordham University School of Law

1) Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It 36 (2010). *See also* Jon Herskovitz, *North Korea 'no longer bound by armistice'*, Indep., May 27, 2009, *available at* http://www.independent.co.uk/news/world/asia/north-korea-no-longer-bound-by-armistice-1691347.html.

2) *North Korea fires seven short-range missiles into the East Sea*, The Hankyoreh (English), July 6, 2009, *available at* http://english.hani.co.kr/arti/english_edition/e_northkorea/364175.html.

on that very same day, in what many news sources regarded as an act of "cyberwarfare,"[3] North Korea sent out a coded message[4] to approximately 40,000 computers,[5] which contained a botnet virus called "MyDoom."[6] Once infected with the North Korean botnet virus, these computers relentlessly flooded the government and private networks of both the United States and the Republic of Korea (hereafter South Korea).[7] The first wave of the North Korean "DDOS"[8] (Distributed Denial of Service) attacks lasted from July 4th to July 9th, and focused primarily on U.S. government and private websites.[9] The second wave of DDOS attacks (July 9th), targeted

---

3) Examples include *North Korea Waging Cyber Warfare?*, CBS NEWS, July 9, 2009, *available at* http://www.cbsnews.com/stories/2009/07/09/world/main5145967.shtml; Ryan Mauro, *North Korea's Cyber War*, FRONTPAGEMAG.COM, July 13, 2009, *available at* http://archive.frontpagemag.com/readArticle.aspx?ARTID=35547. *But see* Sang-Hun Choe & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,* N.Y. TIMES, July 9, 2009, *available at* http://www.nytimes.com/2009/07/09/technology/09cyber.html?adxnnl=1&adxnnlx=1302448132-eezVYpQo8sR6EUEN3ckITw; Ellen Nakashima, Brian Krebs & Blaine Harden, *U.S., South Korea Targeted in Swarm of Internet Attacks,* WASH. POST, July 9, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html (although the article mentions briefly about the "specter of cyberwarfare").

4) Nakashima, Krebs & Harden, *supra* note 3 (the coded message contained a bug called "MyDoom," which told tens of thousands of computers to "repeatedly attempt to access the targeted sites, a tactic aimed at driving up traffic beyond the sites' normal capacity and denying access to legitimate users").

5) CLARKE & KNAKE, *supra* note 1, at 40.

6) A "botnet" is "a large number of compromised computers that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail." *Botnet Definition from PC Magazine Encyclopedia*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=botnet&i=38866,00.asp (last visited April 24, 2011).

7) Richard Lloyd Parry, *North Korea 'launches massive cyber attack on Seoul'*, TIMES, July 9, 2009, *available at* http://www.timesonline.co.uk/tol/news/world/asia/article6667440.ece.

8) A "DDOS" attack is similar to a "DOS" (Denial of Service) attack, which "is designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash." A DDOS attack, however, is more effective, in that a DDOS attack "involves the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the DOS from multiple paths makes backtracking the attack extremely difficult, if not impossible." U.S. ARMY TRAINING AND DOCTRINE COMMAND DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, HANDBOOK NO. 1.02, CYBER OPERATIONS AND CYBER TERRORISM, 24 (2005).

9) CLARKE & KNAKE, *supra* note 1, at 36-37 ("The U.S. websites were hit with as many as 1 million requests per second, choking the servers. The Treasury, Secret Service, Federal Trade Commission, and Department of Transportation web servers were all brought down at some

South Korean networks specifically, with the infected computers attacking dozens of South Korean government and private networks.[10] The third wave (July 10th), however, was by far the most destructive, with the "now estimated 166,000 computers in seventy-four countries [started] flooding the sites of Korean banks and government agencies."[11]

All told, this massive DDOS attack was impressive, with U.S. and South Korean networks being flooded by the millions of requests being sent out by the hundreds of thousands of computers infected with the North Korean botnet virus.[12] In the United States for example, the North Korean DDOS attack targeted the networks of the Department of State, National Security Agency, Department of Homeland Security, White House, NASDAQ, Amazon.com, Yahoo.com, and the New York Stock Exchange, amongst other networks.[13] Likewise, the networks of South Korea's Presidential Office, National Assembly, National Intelligence Service, Chosun news site, Ministry of National Defense, Korea Exchange Banks, and the leading network security firm AhnLab were also attacked.[14][15] In the end, approximately thirty-five major U.S. and South Korean government and commercial websites came under major attack from July 4th, 2009 to July 10th, 2009.[16]

But despite the extent of the attacks, many of the organizations that were targeted were able to recover relatively quickly,[17] returning online

---

point between July 4 and July 9," though the White House web server survived").

10) *Id.* at 37 ("Another 30,000 to 60,000 computers infected with a different variant of the virus were told to target a dozen or more South Korean government sites, Korean banks, and a South Korean Internet security company on July 9").

11) *Id.* (further attacks on the U.S. networks were deemed futile because the government and major corporations were effectively filtering out the attacks).

12) *Id.* at 36-38.

13) Technolytics Institute, Cyber Security Briefing, Cyber Intelligence: North Korea's Cyber Attack 2 (2009).

14) Parry, *supra* note 7.

15) Jane Han, *Cyber Attack Hits Korea for Third Day*, The Korea Times, July 9, 2009, *available at* http://www.koreatimes.co.kr/www/news/biz/2009/07/123_48203.html.

16) Technolytics Institute, *supra* note 13, at 2.

17) Nick Shapiro, a White House Spokesman during these cyber attacks, said in a statement that "[t]he preventative measures in place to deal with frequent attempts to disrupt whitehouse.gov's service performed as planned, keeping the site stable and available to the general public, although visitors from regions in Asia may have been affected." Choe &

within several hours of being shut down.[18] Indeed, when compared to the threat of a nuclear weapon[19] or even a short-range missile, the cyber weapon used by North Korea[20] does not seem so serious.[21] However, to focus on the direct impact of North Korea's cyber attack is to miss the bigger picture — that is, the underlying message encrypted within North Korea's July 4th DDOS attacks.[22] Indeed, former government employee Richard A. Clarke, who was the Deputy Assistant Secretary of State for Intelligence under President Reagan, and Assistant Secretary of State for Political-Military Affairs under President George H. Bush,[23] attests to the seriousness of this DDOS attack in his book *Cyber War: The Next Threat to National Security and What to Do About It*. In this book, Richard A. Clarke points out that, although the damage done to the U.S. and South Korean networks was for the most part contained,

> [I]t was likely only meant as a shot across the bow. What we do know is that there was an agenda and motivation for the attack. This was not a worm simply released into the wilds of the Internet and allowed to propagate. Someone controlled and directed the attack and modified its target list to focus on the more vulnerable Korean sites.[24]

Markoff, *supra* note 3.

18) *Id.*

19) For information on North Korea's nuclear program generally, *see North Korea's Nuclear Program*, N.Y. Times, *available at* http://topics.nytimes.com/top/news/international/countriesandterritories/northkorea/nuclear_program/index.html.

20) Technolytics Institute, *supra* note 13, at 2 (Key Analysis – "This was not a major strike! North Korea's cyber attack demonstrates the accuracy of the capabilities assessed and documented back in March of 2009").

21) For one person's view that North Korea's cyber attacks were blown out of proportion, *see* George Smith, *The Pathetic War: South Korean and US websites suffer cyberattack*, GlobalSecurity.org, July 10, 2009, *available at* http://sitrep.globalsecurity.org/articles/090710413-the-pathetic-war-south-korean.htm.

22) Choe & Markoff, *supra* note 3 ("This is not a simple attack by an individual hacker, but appears to be thoroughly planned and executed by a specific organization or on a state level," the South Korean spy agency, the National Intelligence Service, said in a statement").

23) Richard A. Clarke: Bios, http://www.richardaclarke.net/bio.php (last visited Apr. 27, 2011).

24) Clarke & Knake, *supra* note 1, at 38.

The North Korean DDOS attack, then, can be seen as a mere "throw-away" cyber weapon, whose poor code etiquette and quality was most likely known to those who developed it.[25] It is more likely that North Korea launched the aforementioned cyber attacks in order to show how quickly it could attack the important networks of the U.S. and South Korea, not to mention its ability to elude detection[26] (although the U.S. was reluctant to attribute the attacks to North Korea publicly,[27] South Korea was more than willing to blame its northern neighbor).[28]

Indeed, the July 4th attacks were more than just isolated incidents[29] committed by a country hoping to have its moment in the international spotlight. Rather, the attacks served as strong support for the contention that North Korea is dedicating a considerable portion of its military resources towards cyberwarfare.[30] Specifically, intelligence sources indicate

---

25) Jose Nazario, manager of security research at Arbor Networks, referred to North Korea's July 2009 cyber attacks as a "garden-variety attack," with the code being "pretty elementary in many respects." Choe & Markoff, *supra* note 3.

26) Nakashima, Krebs & Harden, *supra* note 3 ("Experts…cautioned against implicating North Korea too soon").

27) Clarke & Knake, *supra* note 1, at 38 ("The U.S. government has yet to directly attribute the attack to North Korea, though South Korea has not been shy about doing so").

28) Sung Hwee Moon, *Why North Korea is Silent on Cyber Warfare*, DailyNK, July 20, 2009, *available at* http://www.dailynk.com/english/read.php?cataId=nk00400&num=5185 ("The South Korean National Intelligence Service (NIS) asserted at the time that those who backed the attacks were either North Korean or pro-North Korea factions. However, despite such an accusatory assessment, North Korea has not responded in any way."); *US suspects N Korea was behind cyber attacks*, Hindustan Times, July 9, 2009, *available at* http://www.hindustantimes.com/US-suspects-N-Korea-was-behind-cyber-attacks/Article1-430299.aspx ("The US believes North Korea was responsible for a massive cyber attack on government and other websites during the past week, Fox News reported on Wednesday. An unnamed US defence official told Fox the attack targeted dozens of websites, including the ones for the US Defence Department and the Department of State").

29) *See North Korean Hacking Capability 'Penetrating the CIA and the Pentagon is the Standard'*, Sisa Seoul, Oct. 21, 2005; *NKorea operates cyber warfare unit to disrupt SKorea's military command: official*, The Syndey Morning Herald, July 12, 2006; *South Korea PM Warns of Hacking Threat by North Korea, China*, Channel NewsAsia, Oct. 14, 2008, *available at* http://www.channelnewsasia.com/stories/afp_asiapacific/view/382702/1/.html.

30) Steve S. Sin, *Hangukgwa Juhanmigune Daehan Bukhangwa Junggugeurobuteoui Cyber Wihyeop [Cyber Threat Posed by North Korea and China to South Korea and US Forces Korea]*, 364 Gukbanggwa Gisul [Def. & Tech.], 28, 28-33 (2009) (In 2007, North Korea spent an estimated $5.2 billion on cyberwarfare alone).

that North Korea has set up cyberwarfare units aimed at infiltrating the networks of enemy countries.[31] According to Richard A. Clarke, North Korea may have up to four cyberwarfare units[32] at its disposal.[33] But given the secrecy of the North Korean regime, such affirmations regarding the existence of these specialized military units are somewhat tenuous, although the existence of at least some cyberwarfare units (especially Unit 121[34]) has been attested to by various sources.[35] The actual cyberwar threat that North Korea poses to the rest of the world, however, seems to be more of a certainty.[36] A Cyber Security Defense Briefing on North Korea's cyberwar threat, for instance, cited a cyber capabilities threat matrix

---

31) *N. Korea Operates Cyber War Unit*, The Korea Times, May 5, 2009, *available at* http://www.koreatimes.co.kr/www/news/nation/2010/04/113_44358.html ("the General Staff of the North Korean People's Army has been operating for years a 'technology reconnaissance team,' which is exclusively in charge of collecting information and disrupting military computer networks in South Korea and the U.S."); Sin, *supra* note 30 ("North Korea reportedly set up a CW unit in the late 1980s").

32) Clarke & Knake, *supra* note 1, at 43((1) Unit 110, (2) Unit 121 (the KPA's Joint Chiefs Cyber Warfare Unit, which allegedly has over six hundred hackers), (3) the Enemy Secret Department Cyber Psychological Warfare Unit 204 (which according to Mr. Clarke has approximately one hundred hackers, and specializes in cyber elements of informational warfare) and (4) the Central Party's Investigations Department Unit 35 (a "smaller but highly capable cyber unit with both internal security functions and external offensive cyber capabilities")).

33) Sin, *supra* note 30 (According to Sin, "Unit 121 is reportedly subordinate to the Reconnaissance Bureau," based on various open source and media reports. The Reconnaissance Bureau, in turn, is part of the General Staff Department of the Ministry of People's Armed Forces, which is part of the broader National Defense Commission. Such is the suspected Command Structure of the North Korean Armed Forces).

34) *See* Sin, *supra* note 30.

35) *Id.* ("Open source reports refer to two different [cyberwarfare] organizations – the State Security Agency's electronic communications monitoring and computer hacking unit… and the North Korean Ministry of People's Armed Forces (MPAF) CW unit, known as Unit 121" (footnotes omitted)). *See also* Kevin Coleman, *Inside DPRK's Unit 121*, Defensetech.org, Dec. 24, 2007, *available at* http://defensetech.org/2007/12/24/inside-dprks-unit-121/ (The North Korean military created a new unit that focuses solely on cyber warfare. The unit, dubbed Unit 121, was first created in 1998 and has steadily grown in size and capability since then"); *NKorea operates cyber warfare unit to disrupt SKorea's military command: official*, *supra* note 29.

36) *North Korea planning a cyber war?*, The Korea Times, June 1, 2011, *available at* http://www.koreatimes.co.kr/www/news/nation/2011/06/113_88097.html ("[r]ealizing that it takes less money to raise and maintain a cyber war force than an army, navy, and air force, North Korea is concentrating on a prospective cyber war").

(updated in 2009) that ranked North Korea as the 8th biggest threat to the U.S.'s cyber defenses.[37] Steve Sin, meanwhile, a Major in the U.S. Army who was assigned as the Senior Analyst of the Open Source Intelligence Branch, Directorate of Intelligence, U.S. Forces Korea at the time of the writing of his article, emphasized that North Korea possesses "highly developed CW capabilities," that they "continue to develop new and more sophisticated CW arsenals; and have at least tested their capabilities if not already used them in actual attacks against their adversaries."[38]

It is attacks such as these, coupled with North Korea's dedication towards this type of warfare, which lends support to those already concerned with cyberwarfare's destructive potential, including the current Obama Administration.[39] But do the July 4th, 2009 cyber attacks amount to acts of cyberwar? Or are they just another form of espionage (i.e. information gathering), which has been going on between nation states since time immemorial?[40] Even if we were to presume that North Korea committed acts of cyberwar between July 4th, 2009 and July 9th of the same year, under

---

37) Technolytics Institute, *supra note 13, at 1* (Technolytics Institute, July 2009) (The Briefing also cited that North Korea possesses the following offensive cyber weapons: moderately advanced distributed denial of service capabilities, moderate virus and malicious code capabilities, and moderate to strong hacking capabilities, with a limited to moderate experience rating).

38) Sin, *supra* note 30 (In the same article, however, Sin cites a cyber threat matrix which indicates that North Korea has no advanced weapons, though they have limited Intermediate Weapons and basic data weapons (the study was from 2007). *See also* Coleman, *supra* note 35 (assessing the threat which Unit 121 poses in the realm of cyberwar).

39) In June of 2009, a new cyber command – "USCYBERCOM" for short – was approved by Defense Secretary Robert M. Gates to become "a unified, subdivision of U.S. Strategic Command to manage the Defense Department's resources of 15,000 computer networks across 4,000 military bases in 88 countries." Lance Whitney, *U.S. CyberCom launches with first commander*, CNET News, May 24, 2010, *available at* http://news.cnet.com/8301-13639_3-20005749-42.html (Army General Keith Alexander was named as USCYBERCOM's first commander). *See also Fault Lines – Cyberwar*, Al Jazeera (Eng.), Dec. 16, 2010, http://english.aljazeera.net/programmes/faultlines/2010/04/2010421152728872905.html (approx. 13:32-14:49: Lt. General Keith Alexander, the first commander of U.S. CyberCom, states that cyberwar could exist).

40) *A new frontier in cyber war?*, Al Jazeera (Eng.), Oct. 2, 2010, http://english.aljazeera.net/programmes/insidestory/2010/09/201093014161289992 6.html (approx. 8:38-10:29: Rik Ferguson, an SNR Security Advisor for Trend Micro, stated that up until now (Oct. 2010), what we have seen are merely acts of 'cyber espionage', and not warfare).

what body of law would we hold North Korea accountable to? Do the current treaties and bodies of law dealing with war address cyber attacks, or are we in desperate need of a new treaty which would specifically address cyberwarfare?

I will contend in my paper that North Korea's July 4th attacks constituted acts of both war and cyberwar, and that their attacks on U.S. and South Korean government and private networks violated several treaties pertaining to war. Ultimately, the flow of the paper will be as follows: First, I will talk briefly and generally about the law of war, citing relevant international law and confining my argument to the most pertinent documents and principles. Second, I will talk about what constitutes acts of war and cyberwar, breaking each term down into a workable step-by-step analysis. Third, I will apply these definitions to North Korea's attacks, and contend that their attacks on U.S. and South Korean websites in July of 2009 constituted acts of war and cyberwar. Fourth, I will point to the specific treaties which these cyber attacks violated, including the U.N. Charter, Geneva and Hague Conventions. Finally, I will point to new developments in the realm of cyberwarfare, specifically efforts by the U.S. and Russia to come up with a treaty regulating cyberwarfare.

I. The Law of War

The law of war has been in constant development ever since states first came into existence,[41] and as such volumes of treaties,[42] principles,[43]

41) Jeff A. Bovarnick et al., Law of War Deskbook 8, 20 (2010) (Laws of war pertaining to the declaration of war have existed since the times of the ancient Egyptians and Sumerians (25th century B.C.), and laws of war pertaining to the conduct of war have existed since the Ancient Babylonians (7th century B.C.). In the present day, the law of war is defined generally as "a body of international law intended to dictate the conduct of State actors (typically combatants) during periods of conflict").

42) According to the *Yale Law School Avalon Project,* there are over thirty Geneva and Hague treaties alone that deal with the laws of war, from the Declaration of Paris on April 16th, 1856 (regarding maritime law) to the Convention on Prohibiting Biological Weapons, March 26th 1975. The Avalon Project: Documents in Law, History, and Diplomacy,http://avalon.law.yale.edu/subject_menus/lawwar.asp (last visited Apr. 23, 2011).

43) Bovarnick et al., *supra* note 41, at 130 (An example of a principle of the law of war is

quotes,[44] and so forth are available for interpretation and analysis.[45] All these sources of law, in turn, control how every State actor conducts itself during times of conflict, regardless of whether they are a party to a specific treaty or not. This principle is referred to as the "universality" principle of war, which states that all nation-states are bound by the law of war "based on the theory that law of war conventions largely reflects customary law."[46]

Such sources of law attempt to define what constitutes an act of war, how a state may declare war, what is acceptable conduct during war, how prisoners of war are to be treated, and so on.[47] For our purposes, I will confine the study of the law of war to the following: the definition of "war" as stated in the 2010 Law of War Deskbook, the definition of "cyberwar," as stated by Myriam Dunn Cavelty in her article "Cyberwar," the United Nations Charter Article 2(4), the Geneva Convention, Additional Protocol I, Article 48 (1977) and the Hague Cultural Property Convention of 1954, Article 4(1).

---

the "Rendulic Rule," which allows for the destruction of civilian property "if military necessity 'imperatively demands' such action" (quoting from Hague Relations, art. 23(g)).

44) "Be polite; write diplomatically; even in a declaration of war one observes the rules of politeness" – Otto von Bismarck. *See* RIGHT WORDS: TIMELESS WORDS – OTTO VON BISMARCK (1815-1898), GERMAN STATESMAN OF THE 19TH CENTURY, http://www.rightwords.eu/quotes/quote-details/508/be-polite-write-diplomatically-even-in-a-... (last visited April 27, 2011).

45) Generally speaking, Article 38 of the Charter of the International Court of Justice (ICJ) lists the following sources of international law: international agreements (treaties, custom, general principles of law) recognized by civilized nations, judicial decisions, and the teaching of highly qualified scholars of civilized nations. *See* Statute of the International Court of Justice art. 38, Apr. 18, 1946, *available at* http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0.

46) BOVARNICK ET AL., *supra* note 41, at 14 ("Reinforced tenets of *Jus ad Bellum* and *Jus in Bello*…ushered in the era of "universality").

47) *Id.* at 5-6 (The 2010 *Law of War Deskbook* defines the law of war as the "customary and treaty law applicable to the conduct warfare on land and to relationships between belligerents and neutral States" (quoting from the Department of the Army, Field Manual 27-10, The Law of Land Warfare, July 1956)).

II. 'War' & 'Cyberwar', defined

First, it is pertinent to define the terms 'war' and 'cyberwar' themselves, so as to better determine whether North Korea has violated any laws of war.

1. War

First, what constitutes an act of 'war'? Generally, war has been understood as a conflict between two or more nation-states — a struggle of wills[48] involving organized armies at odds with one another for social, political, or even ideological reasons. More specifically, the *Law of War Deskbook*, a three volume piece containing international and operational law subjects taught to military judge advocates, has broken down the concept of war into four elements: "(a) A contention; (b) between at least two nation-states[49]; (c) wherein armed force is employed; (d) with an intent to overwhelm."[50]

2. Cyberwar

In turn, it is important to have a concrete definition of 'cyberwar', one that can be broken down into several elements and analyzed accordingly. Unfortunately, the *Law of War Deskbook* does not define the phrase cyberwar within its pages. A helpful definition of cyberwar, however, can be found in *The Ashgate Research Companion to Modern Warfare*, particularly in an article entitled "Cyberwar" by Myriam Dunn Cavelty (other definitions of cyberwar,

---

48) Carl Von Clausewitz, On War 90-123 (Michael Eliot Howard & Peter Paret ed., Princeton Univ. Press 1976) (1832) ("If . . . we consider the pure concept of war . . . . its aim would have always and solely to be to overcome the enemy and disarm him." This encompasses "three broad objectives, which between them cover everything: destroying the enemy's armed forces; occupying his country; and breaking his will to continue the struggle").

49) The 'nation-state' is a relatively new phenomenon, "a product of strictly modern developments like capitalism, bureaucracy, and secular utilitarianism" – a collection of ethnic groups within strict territorial boundaries who have come together to forge a unique "nationalistic" identity which they are willing to live and die for. Anthony D. Smith, The Ethnic Origins of Nations 8 (2007).

50) Bovarnick et al., *supra* note 41, at 5.

however, do exist[51]).[52] Currently the Dean of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland,[53] Myriam defines cyberwar as referring to the "conducting and preparing [of] military operations according to information-related principles. It features formal military forces pitted against each other, and aims at disrupting the (military) information and communications systems on which the adversaries rely in order to 'know' themselves."[54] Myriam then breaks this down into a step-by-step analysis, stating that an act of cyberwar involves (1) an attack on computer systems[55] by a (2) state actor, with (3) warlike intentions.[56]

---

51) *See also* Bruce Schneier's definition of cyberwar, found in his piece, Bruce Schneier, *Cyberwar: Myth or Reality*, Schneier.com, http://www.schneier.com/essay-201.html (last visited Apr. 26, 2011); Cyberwarfare 2011, *Project of the International Convention on Prohibition of Cyberwar*, Cyberwarfare Blog (Jan. 14, 2011, 12:27 AM), http://cyberwarfare.blog.com/2011/01/14/project-of-the-international-convention-on-prohibition-of-cyberwar/ ("A Ukrainian professor of International Law, Alexander Merezhko, has developed a project called the International Convention on Prohibition of Cyberwar in Internet. According to this project, cyberwar is defined as the use of Internet and related technological means by one state against political, economic, technological and information sovereignty and independence of any other state").

52) Myriam Dunn Cavelty, *Cyberwar, in* The Ashgate Research Companion to Modern Warfare 123, 123-44 (George Kassimeris & John Buckley ed., 2010).

53) Myriam Dunn Cavelty – Welcome, http://www.myriamdunn.com/index/Welcome.html (last visited April 25, 2011) ("Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and Fellow at the 'stiftung neue verantwortung' in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues.").

54) Cavelty, *supra* note 52, at 127-28.

55) '[C]omputer systems' is defined by the Institute for Telecommunication Sciences, the research and engineering branch of the National Telecommunications and Information Administration, as "[a] functional unit, consisting of one or more computers and associated software, that (a) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program, (b) executes user-written or user-designated programs, and (c) performs user-designated data manipulation, including arithmetic and logic operations. Note: A computer system may be a stand-alone system or may consist of several interconnected systems." *See The Institute for Telecommunication Sciences*, Boulder Colorado, *available at* http://www.its.bldrdoc.gov/fs-1037/dir-008/_1198.htm (last visited April 27, 2011).

56) Cavelty, *supra* note 52, at 131.

III. North Korea's July 4th Cyber Attacks Constituted Acts of War and Cyberwar

With the terms "war" and "cyberwar" now defined, it is pertinent to see if North Korea's July 4th cyber attacks fit within these definitions.

1. The July 4th Cyber Attacks Constitute Acts of War

First, did North Korea's cyber attacks constitute acts of war? Using the Law of War Deskbook's definition of war,[57] the following can be said about North Korea's July 4th cyber attacks:

(a) "A contention." There clearly has been hostility between North Korea, South Korea and U.S. Forces Korea ever since the 1953 Korean War Armistice.[58] Indeed, since the signing of the armistice the North Korean army has on several occasions clashed with both South Korea and U.S. Forces Korea,[59] and even went as far as to say in 2009 that it would no longer abide by the armistice.[60] North Korea's resentment and anger towards the U.S. and South Korea (plainly manifested in their propaganda[61]) has served as the backdrop for their prior acts of aggression. Specifically, the circumstances surrounding North Korea's July 4th cyber attacks were the U.S. and South Korea's condemning of North Korea's testing of a nuclear bomb,[62] North Korea's claim that South Korea was spreading false

---

57) Bovarnick et al., *supra* note 41, at 5.

58) Korean War Armistice Agreement, July 27, 1953, *available at* http://www.ourdocuments.gov/doc.php?flash=old&doc=85.

59) Examples of hostilities perpetrated by North Korea include the "Axe Murder Incident" on August 18th, 1976 (Wayne Kirkbride, DMZ: A Story of the Panmunjom Axe Murder (1984)) and more recently the bombardment of Yeonpyeong on November 23rd, 2010 (John Sudworth, *North Korean artillery hits South Korean island*, BBC, Nov. 23, 2010, *available at http://www.bbc.co.uk/news/world-asia-pacific-11818005*).

60) Herskovitz, *supra* note 1.

61) For examples of North Korean propaganda, *see* Hyung-chan Kim & Dong-kyu Kim, Human Remolding in North Korea: A Social History of Education (2005) (propaganda in the North Korean school system).

62) Peter Foster & Malcolm Moore, *World unites to condemn North Korea nuclear test*, The Telegraph, May 25, 2009, *available at* http://www.telegraph.co.uk/news/worldnews/asia/

information about its (North Korea's) involvement in cyberattacks,[63] and a cyber defense drill conducted by the U.S. and South Korea which North Korea saw as an act of aggression.[64] Indeed, North Korea itself saw the events leading up to the July 4th cyber attacks – namely, international condemnation of their testing of a nuclear weapon – as "a declaration of undisguised confrontation and a declaration of a war against the DPRK."[65] The 'contention' prong is therefore satisfied.

(b) "Between at least two nation-states." Though attribution of cyber attacks is an admittedly hard task,[66] the United States and South Korea considered North Korea as a primary suspect in the July 4th cyber attacks.[67] This is based on circumstantial evidence,[68] the history of conflict between North Korea, South Korea and the U.S.,[69] and the knowledge of special cyberwarfare units located within North Korea, who have made it their job

---

northkorea/5383019/World-unites-to-condemn-North-Korea-nuclear-test.html ("US President Barack Obama accused Pyongyang of "directly and recklessly challenging the international community" and seeking to undermine stability in the region." "Japan and South Korea, the two states most immediately threatened by North Korea, also joined the US in condemning the test").

63) Ron Synovitz, *North Korea Suspected in Cyberoffensive Against U.S., South Korea*, Radio Free Europe – Radio Liberty, July 9, 2009, *available at* http://www.rferl.org/content/feature/1773148.html (North Korea also warned of "high-tech war" against the South for spreading what it said was false information about its involvement in cyberattacks).

64) Clarke & Knake, *supra* note 1, at 35 (In June of 2009, an American official publicly announced that the U.S., along with Japan and South Korea (among other nations) would be conducting a cyber war exercise known as 'Cyber Storm', which would test the cyber defense of each country involved in the exercise. Despite the apparent innocence of such an exercise, "North Korean media soon responded by characterizing the pending exercise as a cover for an invasion of North Korea").

65) Colin Mark, *North Korea: Cyber Mad Dogs or Bluster Kings?* DoD Buzz, Apr. 20, 2009, *available at* http://www.dodbuzz.com/2009/04/20/north-korea-cyber-mad-dogs-or-bluster-kings/ (citing Kevin Coleman article).

66) Stewart Baker, Shaun Waterman & George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* 3 McAfee (2009), http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf ("attribution challenges in cyberspace give all attackers 'plausible deniability'").

67) Malcolm Moore, *North Korea blamed for cyber attack on South Korea,* The Telegraph, July 8, 2009, *available at* http://www.telegraph.co.uk/news/worldnews/asia/southkorea/5778176/North-Korea-blamed-for-cyber-attack-on-South-Korea.html; *US suspects N Korea was behind cyber attacks*, Hindustan Times, *supra* note 28.

68) Clarke & Knake, *supra* note 1, at 36-40.

69) *See* Cavelty, *supra* note 52, at 131.

to infiltrate U.S. and South Korean websites.[70] It is more likely than not, therefore, that the cyber attacks were committed by North Korea, satisfying the 'nation-states' prong.[71]

(c) "Wherein armed force is employed." This is arguably the most difficult – and arguably most important prong to satisfy, because if the armed force prong is not met, then a state does not have the right to respond with self-defense.[72] Fortunately, a prominent scholar – Michael N. Schmitt[73] – has laid out six factors to be considered in determining whether a cyber attack constitutes an armed attack.[74] The factors are as follows: (i) severity (scope and intensity of the attack, including "the number of people killed, size of the area attacked, and amount of property damage done"[75]) (ii) immediacy (duration of the attack and the amount of time the effects were felt), (iii) directness (if the cyber attack was the proximate cause of the damage), (iv) invasiveness (whether the attack physically or electronically crosses state borders "and whether it cause[d] harm within the victim-state"[76]) (v) measurability (was the harm primarily quantifiable or merely speculative?), and (vi) presumptive legitimacy (were the cyber attacks part of customary state practice?)[77]

While debatable, one could make a strong argument that North Korea's

---

70) *N. Korea Operates Cyber War Unit*, *supra* note 31.

71) *But see* Lolita C. Baldor, *North Korea a suspect in U.S. cyber attacks*, Army Times, July 8, 2009, *available at* http://www.armytimes.com/news/2009/07/ap_cyber_attacks_north_korea_070809/ ("U.S. authorities eyed North Korea on Wednesday as the origin of the widespread cyber attack that overwhelmed government Web sites in the United States and South Korea, although they warned it would be difficult definitely to identify the attackers quickly"); Malcolm Moore, *supra* note 69 ("There was also speculation in the South Korean media that the attacks may have originated in China").

72) Jeffrey Carr & Lewis Shepherd, Inside Cyber Warfare: Mapping the Cyber Underworld 58 (2010).

73) Michael N. Schmitt is currently the Dean of the College of International and Security Studies at the George C. Marshall European Center for Security Studies, having assumed the position in September of 2008. For more, *see* http://www.marshallcenter.org/mcpublicweb/en/component/content/article/19-cat-bios-faculty/413-art-bio-faculty-schmitt.html?directory=30 (last visited April 26, 2010).

74) Carr & Shepherd, *supra* note 72, at 58-61 (Schmitt's factors are part of a broader "effects-based" test which the authors deem the most acceptable for cyber attacks.)

75) *Id.* at 60.

76) *Id.* at 60-1.

77) *Id.*

cyber attacks were indeed armed. In regards to the first prong (severity), while no one was killed by these cyber attacks, the size of the area attacked – the whole world, specifically the United States and South Korea – was quite substantial. The second prong (immediacy) is fairly weak, in that the effects of the attacks (shutting the sites down) lasted only several hours at a time, although the attacks themselves were spread out over the course of five days. The third prong (directness), however, is clearly met, in that the cyber attacks were the proximate cause of the damage to the U.S. and South Korean networks. The attacks also satisfy the fourth prong (invasiveness), since the attacks electronically crossed state borders and caused harm within the victim-states. The measurability of the harm (fifth prong), however, is somewhat weak, since any damage that was caused was more or less speculative.[78] The sixth and final prong (presumptive legitimacy), though, weighs in favor of labeling the attacks as armed, since flooding a state's network with a botnet virus is not part of any treaty or customary state practice accepted by the international community.

In sum, prongs three (directness), four (invasiveness), and six (presumptive legitimacy) weigh in favor of labeling these attacks as armed, while the second (immediacy) and fifth (measurability) weigh in favor of not calling them armed attacks. The first prong (severity) can go either way, since while no one was killed by the attacks, the size of the area covered by the virus was massive. If we were to weigh this evidence in a light most favorable to the U.S. and South Korea, the 'armed' prong could weigh in favor of the United States and South Korea.

(d) "With an intent to overwhelm." North Korea did intend to "overwhelm" the U.S. and South Korean networks with the DDOS attack, and in fact succeeded in overwhelming their various government and private networks. After all, the purpose of a DDOS attack is to overwhelm a computer network,[79] and North Korea knowingly did this to dozens of U.S.

---

78) In tort law, "[a]n individual cannot be compensated for mere speculative probability of future loss unless he can prove that such negative consequences can reasonably be expected to occur." This could presumably apply in the war context, where a state cannot react in self-defense if it does not suffer any serious tangible injury from an attack. *See* The Free Dictionary – Legal Dictionary: Speculative Damages, http://legal-dictionary.thefreedictionary.com/Speculative+Damages (last visited Apr. 27, 2011).

79) *See supra* note 8.

and South Korean networks over a five-day period. Therefore, the 'overwhelm' prong is satisfied, even though the targeted networks were overwhelmed only momentarily.

2. *The July 4th Cyber Attacks Constitute Acts of Cyberwar*

Next, do the July 4th cyber attacks constitute acts of cyberwar? Using Myriam Dunn Cavelty's definition of cyberwar, the following can be said:

(1) "An attack on computer systems." North Korea's July 4th cyber attacks exclusively targeted foreign computer systems (specifically U.S. and South Korean networks), flooding vital government and private networks to the point where such networks became disabled for extended periods of time. The 'computer systems' prong is therefore satisfied.

(2) "By a state actor." As stated in the 'war' analysis earlier, there is always the problem of attribution.[80] However, as stated in that very same analysis, there is a strong possibility that North Korea was behind the attacks.[81] The 'state actor' prong therefore weighs in favor of a finding that a state actor – North Korea - was involved.

(3) "With warlike intentions." Ascertaining the intentions behind North Korea's cyber attacks is problematic, made worse by the regime's extreme secrecy[82] and unwillingness to take credit for the attacks.[83] However, there

---

80) *See supra* note 64.

81) *US suspects N Korea was behind cyber attacks*, *supra* note 28 ("The US believes North Korea was responsible for a massive cyber attack on government and other websites during the past week, Fox News reported on Wednesday. An unnamed US defence official told Fox the attack targeted dozens of websites, including the ones for the US Defence Department and the Department of State"). *See also* Moon, *supra* note 28 ("The South Korean National Intelligence Service (NIS) asserted at the time that those who backed the attacks were either North Korean or pro-North Korea factions").

82) North Korea's closed-off society has earned it the nickname "The Hermit Kingdom." *See* Donald Macintyre, *Inside the Hermit Kingdom*, TIME, Oct. 24, 2005, *available at* http://www.time.com/time/magazine/article/0,9171,1122059,00.html ("Our group…[was] granted a rare visit to the North by Kim Jong Il's secretive regime). *See also* North Korea – A Day in the Life (Golden Monkey Enterprises 2004) (Product Description: "In this rare look inside North Korea, director Pieter Fleury gained unprecedented access to a country generally cloaked in secrecy").

83) Moon, *supra* note 28 ("The South Korean National Intelligence Service (NIS) asserted

are several aspects of the July 4th attacks which weigh in favor of inferring a warlike intent on the part of North Korea. First, the cyber attacks occurred in conjunction with the launching of six short-range rockets in the Sea of Japan, which the International community saw as a clear act of aggression.[84] Given the community's condemnation of this attack, the circumstances surrounding North Korea's three-day long cyber attack seem all the more profound and aggressive, as opposed to a random, isolated testing of another country's defenses. Second, North Korea did not seek to obtain information from either the U.S. or South Korean government networks, nor from their respective private networks.[85] Rather, the likely aims of the attacks were to shut down U.S. and South Korean online networks, and to let those two countries know that North Korea is capable of a well-coordinated attack capable of targeting their key networks.[86] Indeed, cyber attacks are regarded by some as excellent first-strike weapons in war,[87] and so North Korea's July 4th attacks could be seen as testing the waters for a more significant attack down the line.

Based on this analysis, therefore, it would seem that North Korea's cyber attacks in July of 2009 constituted not only acts of war, but acts of cyberwar as well.

---

at the time that those who backed the attacks were either North Korean or pro-North Korea factions. However, despite such an accusatory assessment, North Korea has not responded in any way").

84) Peter S. Green & Heejin Koo, *North Korea Condemned by UN Over Tests of Ballistic Missiles*, Bloomberg, July 6, 2009, *available at* http://www.bloomberg.com/apps/news?pid=newsarchive&sid=akpzdtQXvnus ("North Korea was condemned by the United Nations Security Council after the government in Pyongyang launched several missiles earlier this month in defiance of UN sanctions imposed after a nuclear test").

85) Nakashima, Krebs & Harden, *supra* note 3 (the cyber attacks "did not involve the theft of sensitive information").

86) Clarke & Knake, *supra* note 1, at 38.

87) Technolytics Institute, *supra* note 13, at 1 ("Most military strategists agree that cyber attacks are an excellent first strike weapon. In these specific circumstances, cyber attacks might be considered by Pyongyang as an appropriate and proportional response to the U.N. Security Council's condemnation and reinforcement of existing sanctions").

IV. As Acts of War and Cyberwar, North Korea's July 4th Cyber Attacks Violated Several Treaties Pertaining to the Law of War

Now that it has been established that North Korea's cyber attacks constituted acts of both war and cyberwar, we can now turn our attention to the specific treaties which these acts of war violated. Specifically, North Korea's cyber attacks violated the following laws of war: U.N. Charter Article 2(4), the Geneva Convention Additional Protocol (AP) I, Article 48, and the Hague Cultural Property Convention of 1954. Even though North Korea is not a party to the last two treaties,[88] the aforementioned "universality" principle controls,[89] so North Korea must conform to the articles in both the Geneva and Hague Conventions listed above.

1. U.N. Charter Article 2(4)

North Korea's cyber attacks violated the most basic principle of war: Article 2(4) of the U.N. Charter, which states that the use of force is illegal.[90] Specifically, Article 2(4) states that all the party members are bound to the idea that they shall "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[91] While this applies to all member states in the sense that they are members to this treaty, this principle also applies as customary law – that is, the use of force by non-member states is strongly discouraged, and

88) North Korea became a member of the United Nations on September 17th, 1991. *See* United Nations: Member States, http://www.un.org/en/members/#d (last visited April 24, 2011). However, North Korea is neither a member of the Geneva Convention Additional Protocol I (*See* International Humanitarian Law – State Parties / Signatories, http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=470&ps=P), nor of the Hague Cultural Property Convention of 1954 (*See* International Humanitarian Law – State Parties / Signatories, http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=400&ps=P).

89) *See supra* note 46.

90) U.N. Charter art. 2, para. 4.

91) *Id.*

may lead to either self-defense or collective action (the latter as authorized by the Security Council[92]). With this understanding of Article 2(4) to the U.N. Charter in mind, it becomes clear that North Korea violated Article 2(4) when it launched its DDOS attack onto U.S. and South Korean networks, in that it used cyber force in order to compromise the territorial integrity of both U.S. and South Korea by intentionally and temporarily disabling their government and private networks.[93] Being that the U.S. and South Korean networks, which were the target of the attacks, are located within their respective territories, it is no stretch to say that the very integrity of these territories was compromised when the North Korean virus entered their States.[94] A country's national defense or parliamentary network being down for hours at a time can have devastating consequences for that country, creating hysteria and opening up their defenses to more conventional attacks. In addition, North Korea does not enjoy either of the two exceptions to the Article 2(4) ban on the use of force: The Security Council's decision to take action (Article 39), and the right of every country to self-defense (Article 51).[95]

2. Geneva Convention, Additional Protocol I, Art. 48

Having established that North Korea's cyber attacks clearly constituted a use of force against the territorial integrity of both the U.S. and South Korea, we must now look at the nature of the attacks themselves. Did the cyber attacks only target specific government networks pertinent to achieving a specific military objective, or did the attacks indiscriminately attack innocent civilian objects? The principle of targeting only combatants and military targets, and not civilians or their property, is set forth in Additional Protocol I, Article 48 of the Geneva Convention (1977).[96] Specifically, the article states that "[p]arties to the conflict shall at all times

92) *Id.* art. 51.

93) Choe & Markoff, *supra* note 3.

94) *Id.*

95) U.N. Charter art. 39, 51; Clarke& Knake, *supra* note 1, at 35.

96) Bovarnick et al., *supra* note 41, at 139 (the principle of discrimination is considered the "grandfather of all principles," "form[ing] the foundation for much of the Geneva Tradition of the law of war").

distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[97] Here, North Korea failed to distinguish between military objectives and civilian objects, for in addition to targeting such U.S. networks as whitehouse.gov (White House), state.gov (State Department), dot.gov (U.S. Department of Transportation), nyse.com (the New York Stock Exchange, arguably an indispensable private network[98]), and such South Korean networks as www.mofat.go.kr (Foreign Affairs), www.assembly.go.kr (Republic of Korea National Assembly), and Banking.nonghyup.com (NACF banking), North Korea also attacked yahoo.com (a search engine and news website), blog.naver.com (a popular South Korean blog site[99]), and amazon.com (site for buying books, products, etc.), private websites whose relevance to an attack on U.S. and South Korean government websites seems extremely tenuous.[100] Indeed, a valid military objective can never include attacking the public's morale,[101] whether this means inconveniencing a writer wishing to post a poem on his

97) International Committee of the Red Cross [ICRC], Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S 3.

98) Though one may think that attacking the New York Stock Exchange, which deals with world markets, would also hurt North Korea, North Korea's economy is for the most part closed off from the rest of the world. *See* CIA – The World Factbook: North Korea, https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html (last visited April 26, 2011) ("North Korea, one of the world's most centrally directed and least open economies, faces chronic economic problems."). *See also* Kongdan Oh & Ralph Hassig, *North Korea in 2009: The Song Remains the Same,* 50 Asian Survey 89, 90 (2010) ("the appearance of markets outside the largely defunct state distribution system has been reluctantly condoned by the regime as a "temporary measure" to tide the economy over until socialism somehow gets back on track").

99) Choe & Markoff, *supra* note 3 ("In South Korea, at least 11 major sites have slowed or crashed since Tuesday, including…the top Internet portal Naver.com, according to the government's Korea Information Security Agency").

100) *Naver, auctions, access problem, the secrets of the Blue House*, Kulkaet play blog (July 8, 2009, 8:9 AM), *available at* http://translate.google.com/translate?hl=en&sl=ko&u=http://xcoolcat7.tistory.com/520&ei=hcJTStWNC43UtgOVyYzlBw&sa=X&oi=translate&resnum=1 (last visited April 25, 2011).

101) Hamilton DeSaussure, *Military Objectives,* Crimes of War, http://www.crimesofwar.org/thebook/military-objective.html (last visited April 27, 2011) ("the civilian population must never be the object of attack, making it clear that morale or terror-bombing tactics are clearly a war crime today").

blog, or a businessman trying to read the latest news before work. Ultimately, North Korea's cyber attacks failed to distinguish between civilian and military objects, unnecessarily affecting civilians in the course of attacking the U.S. and South Korea.

3. Hague Cultural Property Convention of 1954

In targeting the private networks of the U.S. and South Korea, North Korea inevitably attacked the cultural property of both countries. Attacking the cultural property of any country is in violation of the Hague Cultural Property Convention of 1954,[102] which demands that its member parties "undertake to respect cultural property situated within their own territory as well as within the territory of other High Contracting Parties by refraining from any use of the property…for purposes which are likely to expose it to destruction or damage in the event of armed conflict."[103] In turn, the term 'cultural property' (as defined in the Convention) includes "movable or immovable property of great importance to the cultural heritage of every people, such as…works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above."[104] Although this Convention was adopted in 1954, the definition of cultural property is broad enough to apply to websites,[105] in that a website can be considered a "movable" piece of property which is "of great importance to the cultural heritage of every people,"[106] particularly persons living in the U.S. and

---

102) The actual, longer name of the treaty is the "1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict and the Regulations for the Execution of the Convention." Roger O'Keefe, The Protection of Cultural Property in Armed Conflict 93(2006).

103) The Hague, 14 May 1954, 249 U.N.T.S 240, Art. 4(1) (For an exception, see subsection (2)).

104) *Id. art. 1(a).*

105) Cyberwarfare 2011, *supra* note 52 ("Professor Merezhko's project suggests that the Internet ought to remain free from warfare tactics and be treated as an international landmark. He states that the Internet (cyberspace) is a 'common heritage of mankind'").

106) The Hague, 14 May 1954, 249 U.N.T.S 240, Art. 1(a).

South Korea.[107] Many websites, including the ones attacked by North Korea in July of 2009, facilitate the viewing and purchasing of a myriad of artistic works, such as books, poems, and editorials, and even fine prints of paintings.[108] Even blog sites often times contain literary works, including poems, short stories, social and political commentaries, and so on.[109] Applying this interpretation of the definition of cultural property to the July 2009 cyber attacks, then, it can be said that North Korea is in violation of Article 4(1) of this Convention, in that North Korea exposed U.S. and South Korean cultural websites to destruction and damage (extended periods of downtime), and otherwise committed acts of hostility towards them.[110] Specifically, North Korea's cyber attacks targeted the following cultural websites of South Korea: Blog.naver.com (a popular blogging site[111]) Mail.naver.com, chosun.com (one of the most popular news websites[112]) and auction.co.kr.[113] The North Korean cyber attacks also

---

107) As implied by Professor Merezhko (*see supra* note 51), cyberspace should be protected as a "common heritage of mankind" (*see supra* note 51). Indeed, websites such as Naver.blog and yahoo.com can be accessed by users from all over the world, with each individual contributing to what is referred to as the "cyberculture," which has been defined as "the culture that emerges from the use of computers for communication and entertainment and business" (though sites such as blog.naver are accessed primarily in their country of origin). *See Cyberculture*, DICTIONARY.COM, *available at* http://dictionary.reference.com/browse/cyberculture (last visited April 27, 2011).

108) From amazon.com, one can buy a copy of "Nineteen Eighty-Four" by George Orwell, a fine art print of "Nympheas" by Claude Monet, and The Poetry of Robert Frost: The Collected Poems, Complete and Unabridged. Likewise, one can access a myriad of editorials from the washingtonpost website

109) Blog.naver.com, for example, contains social commentary articles, ranging from movie reviews to deeper articles concerning the views of a generation, to the fashion world and video game reviews. (Naver, *available at* http://translate.google.com/translate?js=n&prev=_t&hl=en&ie=UTF-8&layout=2&eotf=1&sl=ko&tl=en&u=http%3A%2F%2Fsection.blog.naver.com%2F (last visited April 26, 2011)).

110) The Hague, 14 May 1954, 249 U.N.T.S 240, Art. 1(a) (An exception to this article is listed in subsection 2 of the same article, which states that "[t]he obligations mentioned in paragraph I of the present Article may be waived only in cases where military necessity imperatively requires such a waiver." Here, however, there was no indication that attacking the U.S. and South Korean private websites was a military necessity).

111) *See supra* note 97.

112) Choe & Markoff, *supra* note 3 ("In South Korea, at least 11 major sites have slowed or crashed since Tuesday, including… the mass-circulation newspaper Chosun Ilbo").

113) *Supra* note 100.

targeted the following U.S. websites: yahoo.com, washingtonpost.com, usactionslive.com, and amazon.com.[114] Sites such as washingtonpost.com and chosun.com are obvious cultural institutions, as they contain thousands of news reports and editorials regarding our contemporary world. In addition, blogging sites such as Blog.naver.com often contain works of cultural merit, as mentioned above. North Korea's cyber attacks, therefore, violated the Hague Cultural Property Convention of 1954.[115]

V. Conclusion

Despite the labeling of North Korea's July 2009 cyber attacks on U.S. and South Korean networks as acts of war and cyberwar, which in turn violated at least three treaties pertaining to the law of war, it is unlikely that any state would be willing to go to war over a relatively modest DDOS attack which shuts down their top government and private networks for a few hours. If South Korea, for instance, were to send troops into North Korea because chosun.com or their National Assembly website was rendered inaccessible for part of the day, they would have trouble garnering support from the international community. The same would likely hold true for the United States.

But labeling these attacks as acts of war and cyberwar has its benefits. For one, it exposes these attacks for what they truly are, as opposed to dismissing them as harmless acts that will never amount to the sort of threat that conventional warfare poses.[116] It also gives the international

---

114) *See Id.*

115) The Convention also states, in Article 6, that "[i]n accordance with the provisions of Article 16, cultural property may bear a distinctive emblem so as to facilitate its recognition." This is not necessary in cyberspace, however, where website addresses clearly indicate the contents of the website itself. *But see* Karl Rauscher & Andrey Korotkov, *First Joint Russian-U. S. report on Cyber Conflict*, EastWest Inst., Feb. 3, 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict (U.S. – Russian Joint Resolution states, among other things, that identifying civilian property in cyberspace is difficult).

116) Prasun Sonwalkar, *Cyber war? Not possible, says a study*, Rediff.com: Business, Jan. 18, 2011, http://www.rediff.com/business/slide-show/slide-show-1-tech-cyber-war-not-possible-says-a-study/20110118.htm (A "study by Dr Ian Brown of the Oxford Internet Institute, University of Oxford, and Professor Peter Sommer of the London School of

community – specifically the U.N. – a stronger basis for condemning such attacks. If the attacks are properly labeled as acts of war, the Security Council would have a stronger case for publicly condemning the attacks, and could pursue a course of action with greater international approval. Specifically, the U.N. could pursue two short-term courses of action:

First, if the Security Council of the United Nations were to come out and condemn such cyber attacks as acts of war or cyberwar, or at the very least condemn the attacks in of themselves, this could deter North Korea from launching cyber attacks in future.[117] After all, despite what the North Korean Government may tell its people, its country is largely dependent on foreign aid to feed its people,[118] and so it must balance two aims: showing the rest of the world that it is an international force to be taken seriously, and feeding its people so as to maintain stability within the country.

Second, the U.N. Security Council could pass a Resolution imposing sanctions on North Korea for launching such cyber attacks. The Security Council has done this with respect to North Korea's testing of nuclear weapons, imposing a series of commercial and economic sanctions on North Korea when it passed the United Nations Security Council Resolution 1718 on October 14th, 2006,[119] in response to North Korea's claimed test of a nuclear weapon one week earlier.[120] The Security Council

---

Economics concludes that it is highly unlikely there will ever be a pure 'cyber war' fought solely in cyberspace with *equivalent effects* to recent wars in Afghanistan, the Balkans or West Asia" (emphasis added)) .

117) The U.N. did, however, impose sanctions on North Korea in October 2007, when it tested its first "logic bomb." The testing of this cyber weapon led to a UN Security Council resolution banning sales of mainframe computers and laptop PCs to the East Asian nation." Coleman, *supra* note 35.

118) CIA World Factbook: North Korea – Economy, https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html (last visited April 26, 2011) ("Large-scale international food aid deliveries have allowed the people of North Korea to escape widespread starvation since famine threatened in 1995, but the population continues to suffer from prolonged malnutrition and poor living conditions").

119) Security Council Condemns Nuclear Test by Democratic People's Republic of Korea, Unanimously Adopting Resolution 1718 (2006): Action Prevents Provision of Nuclear Technology, Large-Scale Weapons, Luxury Goods to Country; Permits Inspection of Cargo to Ensure Compliance. Security Council, SC/8853, (Oct. 14, 2006), *available at* http://www.un.org/News/Press/docs/2006/sc8853.doc.htm.

120) *North Korea claims nuclear test*, BBC, Oct. 9, 2006, *available at* http://news.bbc.

could pass a similar Resolution that would, say, impose cyberspace sanctions on North Korea for launching such destructive cyber attacks in the future, which would have the dual effect of punishing North Korea for its acts of war, and creating international awareness regarding North Korea's cyberwarfare front.

While reacting to the attacks in the short-term is important, a long-term course of action is crucial in ensuring a prompt and appropriate response to possible cyberwar attacks in the future. Recently, the United States and Russia came together to draft the first joint Russian-American report on cyber conflicts.[121] Released by the EastWest Institute on February 2011, the report aims primarily at ensuring the protection of civilians during times of war, as put forth in the Geneva and Hague Conventions.[122] The report points out the problems with these two treaties when applied to cyberwar, including the problem of identifying civilian property in cyberspace, determining which "weapons" in cyberwar should be banned, the fact that many cyber warriors are often non-state actors, and the difficulty in coming up with an agreed upon definition of cyberwar.[123]

The step taken by the United States and Russia is an important one. Indeed, relying on conventional treaties in dealing with acts of cyberwar is a difficult task, with necessary reliance on scholarly definitions of terms instead of looking at any one treaty or principle. And although it was possible through the current law of war to define a specific act as an act of war and cyberwar, it would be considerably easier if there was a cyberwar treaty directly on point, putting forth concrete definitions for 'cyberwar' and 'armed cyber-attack.' A cyberwar treaty could also deal with the problem of attribution, what networks may and may not be attacked, which cyber weapons cannot be used, and so on. If the United Nations could propose and pass a treaty[124] which would deal specifically with cyberwarfare,

---

co.uk/2/hi/6032525.stm.

121) Rauscher & Korotkov, *supra* note 115.

122) *See Id.*

123) Karl Rauscher & Andrey Korotkov, *The Russia-U.S. Bilateral on Critical Infrastructure Protection: Working Towards Rules for Governing Cyber Conflict & Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Inst., 7-8 (Feb. 4, 2011), http://issuu.com/ewipublications/docs/us-russia-cyberspace.

124) Tim Gray, *U.N. telecom boss warns of pending cyberwar. Wants cross-continent*

then determining whether certain acts in cyberspace constitute acts of war will become an easier task, and will better guide how the U.N. – and the country attacked – can respond. Such would be the goal of an international cyberwar treaty, which would be dealing with an area of war hardly known by the public at large, and whose grave potential for destruction has been attested to by only a few.

KEY WORDS: Cyberwarfare, Cyberwar, Cyber Attacks North Korea, Democratic People's Republic of Korea, DPRK, DDOS, Distributed Denial of Service Attack, July 4th 2009 Cyber Attacks, Acts of War, Attribution of Cyber Attacks, U.N., Hague Convention on Cultural Property, U.N. Charter Article 2(4), Laws of War, Republic of Korea, South Korea, ROK, United States of America, U.S., Cyberwar treaty, Cyberwarfare treaties

Manuscript received: Oct. 24, 2011; review completed: Nov. 24, 2011; accepted: Dec. 2, 2011.

---

contingency plans in event of large-scale cyberattacks, MSNBC, Sep. 9, 2010, *available at* http://www.msnbc.msn.com/id/39102447/ns/technology_and_science-security/ ("The United Nation's Telecommunications chief is warning nations to join together in developing a coherent global cybersecurity peace treaty or face the very real possibility of an all-out cyberwar").